



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/741,798	12/19/2003	Susan Pittman Dark	58895/P001C1/10316486	5599
29053	7590	04/01/2009	EXAMINER	
FULBRIGHT & JAWORSKI L.L.P			RUTKOWSKI, JEFFREY M	
2200 ROSS AVENUE			ART UNIT	PAPER NUMBER
SUITE 2800			2419	
DALLAS, TX 75201-2784				

MAIL DATE	DELIVERY MODE
04/01/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/741,798	DARK, SUSAN PITTMAN	
	Examiner	Art Unit	
	JEFFREY M. RUTKOWSKI	2419	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 05 January 2009.
- 2a) This action is **FINAL**. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-30,32-50 and 52-74 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-30,32-50 and 52-74 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|----------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ . |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____. | 6) <input type="checkbox"/> Other: _____ . |

DETAILED ACTION

Claims 31 and 51 have been cancelled.

Claim Rejections - 35 USC § 112

1. The following is a quotation of the first and second paragraphs of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. **Claims 1-11 and 33-47** are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. The specification does not adequately describe how the information of a receiving device is gathered.
3. **Claims 17-22 and 26-27** are rejected under 35 U.S.C. 112, first paragraph, as being a single means (system for tracking data flow) claim.
4. **Claims 4, 8, 19, 29, 36, 49 56 and 68** are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The original specification does not adequately describe how parameters are dynamically changed based upon current system operation.
5. **Claims 3 and 8** are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

6. For **claim 3**, it is not clear what type(s) of limits are being set.
7. For **claim 8**, it is not clear what is meant by dynamically changing gathered information based on currently gathered information.
8. **Claims 32 and 52-53** are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for being dependent upon cancelled **claims 31 and 51** respectively.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

10. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

11. **Claims 1-3, 8-9, 11, 15-18, 22, 26-28, 32-35, 40-41, 44-45, 47-48, 52-55, 59, 63-67 and 74** are rejected under 35 U.S.C. 103(a) as being unpatentable over Gleichauf et al. (US Pat 6,415,321), hereinafter referred to as Gleichauf in view of Eschelbeck et al. (US Pat 6,611,869), hereinafter referred to as Eschelbeck and Smith et al. (“Operating Firewalls Outside the LAN Perimeter”).

12. For **claims 1, 33 and 65**, Gleichauf discloses a network environment where packets that are received over the Internet (temporally available network) is received at a router **14** (gateway router) that serves the purpose of directing packets via firewall **16** to either a web server **30** or a file server **34** (receiving devices) based upon address information [**col. 4 line 67 to col. 5 line 15**]. Gleichauf's network environment further includes an Intrusion Detection System (IDS) **18** and a domain mapping system **46** [**figure 3**]. The domain mapping system **46**, which is part of a monitoring system, has an acquisition engine **48** that is used to gather operational information which, inter alia, includes such as Operating System (OS) type, services offered and potential vulnerabilities, on network devices (receiving devices). The information is gathered by the acquisition engine **48** via actively querying the network devices, polling or having the network devices push information [**col. 5 line 45 to col. 6 line 30**].

13. Gleichauf discloses the IDS **18** uses the information stored in the domain mapping system **46** to provide protection for the network devices, such as file server **34** [**col. 6 lines 48-65**]. Gleichauf does not disclose what happens if the IDS **18** detects an attack. Eschelbeck discloses when an attack is detected by an IDS, a message is sent to the firewall via network (feedback network) to have the firewall update it's Access Control List (ACL) (modify operational characteristics) to prevent traffic from the source of the attack from entering the network [**col. 6 lines 4-25**]. It would have been obvious to a person of ordinary skill in the art at the time of the invention to use Eschelbeck's IDS in Gleichauf's invention to provide an active security management environment [**Eschelbeck, abstract**].

14. The combination of Gleichauf and Eschelbeck disclose the active security management of a firewall. The combination of Gleichauf and Eschelbeck do not disclose the active security

management of a gateway router. Smith discloses traditionally routers performed firewall functions via ACL [**Section 1 2nd paragraph**]. Smith also discloses the use of gateway-firewalls to protect networks [**Section 3, Section 3.4 last paragraph**]. It would have been obvious to a person of ordinary skill in the art at the time of the invention to perform active security management on the ACL of a gateway router in Gleichauf's invention to block attacks as close to the source of the attack as possible [**Section 3, 2nd paragraph**].

15. Specifically for **claim 65**, Gleichauf discloses the IDS **48** can be placed in any location in the network, including a firewall [**col. 5 lines 10-13**]. Which suggests an architecture where packets are stored (database for future delivery) and then scanned before being transferred to the destination device.

16. For **claims 2, 34 and 66**, Gleichauf discloses that Simple Network Management Protocol (SNMP) queries (certain data contained in one or more messages) can be used to gather information [**col. 6 lines 23-25**].

17. For **claims 3, 18, 35, 55 and 67**, Gleichau discloses the use of signature matching, where packets are compared to "attack signatures" (pre-established criteria), and pattern matching are known methods to detect attacks [**col. 1 lines 25-30**].

18. Gleichau does not disclose setting limits. Smith suggests the setting of limits by disclosing an firewall and IDS system that detects Denial-of-Service attacks [**Section 1 page 494**]. Since DoS attacks work by causing a victim device to overflow its buffers by sending a large number of requests in a short amount of time, it would have been obvious to a person of ordinary skill in the art at the time of the invention to set limits based on attack signatures (pre-established criteria) to stop a DoS attack before the victim device "crashes".

19. Glecichau also does not disclose adjusting ACL rules when an DoS attack is detected. Smith discloses a system that detects DoS attacks and routers traditionally performed firewall functions via ACL [**Section 1 page 494, Section 1 2nd paragraph**]. It would have been obvious to a person of ordinary skill in the art at the time of the invention to perform active security management on the ACL of a gateway router based upon set limits in Gleichauf's invention to block attacks as close to the source of the attack as possible [**Section 3, 2nd paragraph**].

20. For **claim 8**, Gleichau's invention takes into account that information changes dynamically by actively collecting information from network devices [**col. 5 line 45 to col. 6 line 30**].

21. For **claims 9 and 41**, Gleichauf does not disclose the blocking of certain packets from reaching a destination. Eschelbeck discloses ACL is updated to prevent any more traffic from the source of the attack from entering the network [**col. 6 lines 4-25**]. It would have been obvious to a person of ordinary skill in the art at the time of the invention to use Eschelbeck's IDS in Gleichauf's invention to provide an active security management environment [**Eschelbeck, abstract**].

22. For **claims 11 and 74**, Gleichau suggests an **IDS 18**, which is part of a monitoring system, that can be used to monitor traffic leaving a network device (receiving device) because the **IDS 18** monitors network traffic as a whole [**col. 5 lines 5-8, figure 3**].

23. Gleichau does not disclose a gateway router where the ACL is modified according to outbound traffic. Smith contemplates the use of outbound traffic gateway firewalls [**Section 4**]. Given that Smith is concerned with stopping attacks as close to the source as possible and ACLs

are used to keep one node from accessing another node [**Sections 1 and 3.4**], it would have been obvious to a person of ordinary skill in the art at the time of the invention to block egress traffic via router gateway ACL to prevent an attack from the inside of the network.

24. For **claims 15, 27, 45 and 64**, Gleichauf does not disclose changing ACL rules in a remote system. Smith discloses that in a corporate network, when a firewall detects an attack, messages are sent to remote gateway-firewalls (remote communication system) to have the attacker blocked (modify operational characteristics) [**Section 3.4**]. It would have been obvious to a person of ordinary skill in the art at the time of the invention to perform remote ACL management of a gateway router in Gleichauf's invention to block attacks as close to the source of the attack as possible [**Section 3, 2nd paragraph**].

25. For **claims 16 and 52-53**, Gleichauf discloses the use of an enterprise system [**figure 3**].

26. For **claims 17, 28, 48 and 54**, Gleichauf discloses an IDS **18** (system for tracking data flow; means for real time review) that is used to perform a pattern matching (identification of a specific data pattern; means for comparing) [**col. 1 lines 25-30, figure 3**].

27. Gleichauf discloses the IDS **18** uses the information stored in the domain mapping system **46** to provide protection for the network devices, such as file server **34** [**col. 6 lines 48-65**]. Gleichauf does not disclose what happens if the IDS **18** detects an attack. Eschelbeck discloses when an attack is detected by an IDS, a message is sent to the firewall via network (send instructions from time to time; means for feeding) to have the firewall update its ACL to prevent traffic from the source of the attack from entering the network [**col. 6 lines 4-25**]. It would have been obvious to a person of ordinary skill in the art at the time of the invention to use

Eschelbeck's IDS in Gleichauf's invention to provide an active security management environment [**Eschelbeck, abstract**].

28. The combination of Gleichauf and Eschelbeck disclose the active security management of a firewall. The combination of Gleichauf and Eschelbeck do not disclose the active security management of a gateway router (control device). Smith discloses traditionally routers performed firewall functions via ACL [**Section 1 2nd paragraph**]. Smith also discloses the use of gateway-firewalls to protect networks [**Section 3, Section 3.4 last paragraph**]. It would have been obvious to a person of ordinary skill in the art at the time of the invention to perform active security management on the ACL of a gateway router in Gleichauf's invention to block attacks as close to the source of the attack as possible [**Section 3, 2nd paragraph**].

29. For **claims 22 and 59**, Gleichauf discloses the use of an hypercube storage **50** (database).

30. For **claims 26, 32 and 63**, figure 3 of Gleichauf shows the gateway router **14** of the local site (gateway unique to a particular location) is the gateway router whose ACL is modified

31. For **claim 40**, Gleichau discloses a pattern analysis technique where packets are compared to "attack signatures" [**col. 1 lines 25-30**].

32. For **claim 44**, figure 3 of Gleichauf shows the gateway router **14** of the local site (particular location) is the gateway router whose ACL is modified.

33. For **claim 47**, Gleichauf discloses gathered network information is stored in a hypercube storage **50** [**figure 3**].

34. **Claims 5, 21, 37, 58 and 69** are rejected under 35 U.S.C. 103(a) as being unpatentable over Gleichauf in view of Eschelbeck and Smith as applied to **claims 3, 18, 28, 35 and 67 respectively** above, and further in view of Kouznetsov (US Pat 6,725,377).

35. For **claims 5, 21, 37, 58 and 69**, the combination of Gleichauf, Eschelbeck and Smith does not disclose the manual adjustment of thresholds. Kouznetsov discloses a user decides which attack signatures are to be included in the profile, which results in a manual adjustment of detection thresholds [**col. 2 lines 53-65**]. It would have been obvious to a person of ordinary skill in the art at the time of the invention to use manually adjusted limits in Gleichauf's invention to take into account new attack patterns [**Kouznetsov, abstract**].

36. **Claims 6-7, 10, 12-14, 20, 23-25, 38-39, 43, 46, 57, 60-62, 70-73** are rejected under 35 U.S.C. 103(a) as being unpatentable over Gleichauf in view of Eschelbeck and Smith as applied to **claims 1, 17, 18, 29, 33 and 65 respectively** above, and further in view of Conklin et al. (US Pat 5,991,881) hereinafter referred to as Conklin.

37. For **claims 6, 38 and 70**, the combination of Gleichauf, Eschelbeck and Smith discloses the gathering of information from a network device. The combination of Gleichauf, Eschelbeck and Smith does not disclose the statistical comparison of gathered information. Conklin discloses a attack detection process where captured packets (gathered information) is compared against historical information that was collected over time [**col. 7 lines 50-55**]. It would have been obvious to a person of ordinary skill in the art at the time of the invention to use Conklin's detection mechanism in Gleichauf's invention to use of artificial intelligence to detect attacks [**Conklin, col. 7 line 53**].

38. For **claims 7, 20, 39, 57 and 71**, the combination of Gleichauf, Eschelbeck and Smith does not disclose the gathering of statistics to reflect normal behavior. Conklin disclosure that artificial intelligence techniques can be used to detect attacks, suggests gathering statistics to reflect normal behavior [**col. 7 lines 50-55**]. It would have been obvious to a person of ordinary

skill in the art at the time of the invention to collect statistics to reflect normal behavior in Gleichauf's invention to "feed" the artificial intelligence engine.

39. For **claims 10, 43 and 73**, the combination of Gleichauf, Eschelbeck and Smith does not disclose the storage of received packets. Conklin discloses an IDS process where incoming packets is stored [**figure 7**]. It would have been obvious to a person of ordinary skill in the art at the time of the invention to use Conklin's detection mechanism in Gleichauf's invention to use of artificial intelligence to detect attacks [**Conklin, col. 7 line 53**]. It would have been obvious to a person of ordinary skill in the art at the time of the invention to store packet information in Gleichauf's invention to allow for the use of artificial intelligence to detect attacks [**Conklin, col. 7 line 53**].

40. For **claims 12, 23, 46 and 60**, the combination of Gleichauf, Eschelbeck and Smith does not disclose gathering packet information. Conklin discloses packets are collected and statistical information from the packets is stored (information about the history of the packets) [**figure 7**]. It would have been obvious to a person of ordinary skill in the art at the time of the invention to gather packet information in Gleichauf's invention to use artificial intelligence to detect an attack.

41. For **claims 13, 24 and 61**, Gleichauf discloses the storing information to be used by an IDS **18** system [**col. 6 lines 50-55, figure 3**].

42. For **claims 14, 25 and 62**, Gleichauf discloses the IDS **18** obtains a vulnerabilities list (selected data) that is grouped by OS (parameters of receiving device) and incidence [**col. 6 lines 62-65**].

43. For **claim 72**, Gleichauf discloses a pattern analysis technique where packets are compared to "attack signatures" [col. 1 lines 25-30].

44. **Claims 30 and 50** are rejected under 35 U.S.C. 103(a) as being unpatentable over Gleichauf in view of Eschelbeck, Smith and Kouznetsov as applied to **claims 29 and 49 respectively** above, and further in view of Conklin.

45. For **claims 30 and 50**, the combination of Gleichauf, Eschelbeck, Smith and Kouznetsov does not disclose the gathering of statistics to reflect normal behavior. Conklin disclosure that artificial intelligence techniques can be used to detect attacks, suggests gathering statistics to reflect normal behavior [col. 7 lines 50-55]. It would have been obvious to a person of ordinary skill in the art at the time of the invention to collect statistics to reflect normal behavior in Gleichauf's invention to "feed" the artificial intelligence engine.

Response to Arguments

46. The argument with respect to the gathering of information pertaining to the operation of the receiving device by a monitoring system is not persuasive. While the specification does discuss the gathering of incoming information, the specification does not describe how information is gathered pertaining to the operation of the receiving device or particular location is performed. For example, figure 1 shows incoming packets are gathered and paragraph 0025 discusses packet inspection of the incoming packets. However, the specification does not describe gathering information that pertains to the operation of the receiving device or a particular location.

47. The argument with respect to single means rejection is not persuasive. The claimed invention has undue breadth because it is drawn to an apparatus (monitor system) with a single part (system for data flow tracking).

48. The argument with respect to the Smith reference only being directed to gateway firewalls and not gateway routers is not persuasive. Gleichauf discloses the use of gateway routers [**figure 3**]. As pointed out by the Applicant, Smith discloses a gateway router can also act as a firewall [**page 17 of Applicant's response**].

49. The argument with respect to Smith not disclosing modifying the operating characteristics of a gateway router is not persuasive. This feature was cited as being taught by Eschelbeck.

50. The argument with respect to the prior art not suggesting the modification to a gateway router operation as being a function of data passing through the router is not persuasive. The modification to the operating characteristics of the gateway router is based on the information that pertains to the operation of a receiving device, not traffic flow. The combination of Gleichauf and Eschelbeck was cited as disclosing this feature.

51. The argument with respect to the prior art not showing where arriving data is stored for an amount of time dependent upon data flow situations is not persuasive. Gleichauf discloses the use of signature analysis. In this situation, the packets are stored as long as is needed for a comparison to "attack signatures" are performed [**col. 1 lines 25-30**].

52. Applicant's arguments filed on 01/05/2009 have been fully considered but they are not persuasive, for the reasons stated above.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Ilgun ("USTAT: A Real-time Intrusion Detection System for UNIX") discloses an IDS that analyzes traffic based on real-time information.

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEFFREY M. RUTKOWSKI whose telephone number is (571)270-1215. The examiner can normally be reached on Monday - Friday 7:30-5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Hassan Kizou can be reached on (571) 272-3088. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Jeffrey M Rutkowski
Patent Examiner
03/26/2009

/Hassan Kizou/
Supervisory Patent Examiner, Art Unit 2419